Cancer Epidemiology Unit (CEU)

# Information Security Policy

Version 1.1

# 1 Version history

| Version | Author(s) | Date | Description/changes |
|---|---|---|---|
| 1.0 | Lucy Wright | 8 Oct 2014 | Initial version adapted from CTSU policy |
| 1.1 | Dave Ewart | 29 Apr 2015 | Changes to ensure applicable to CEU, CTSU-specific content removed, CEU-specific content added. |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

# 2 Document storage, availability and change control procedure

Approved versions of this document are kept on the shared drive v:\IG_policies

Routine review and alteration is the responsibility of the IT & Information Security Manager.

Approval of the document is the responsibility of the Information Governance Committee.

Copies may be made available to others (e.g. regulatory agencies, collaborators) as required.

# 3 Approvals

Approvals will be given and recorded on the document.

# 4 Table of Contents

# 5 Definitions

- "NDPH" – The Nuffield Department of Population Health
- "CEU" – Cancer Epidemiology Unit (a part of the NDPH).
- "Information Asset" – a unit of data [e.g. a research study database.]
- "Information Asset Owner" (IAO) – the CEU person responsible for the individual asset [Generally, this is the Principal Investigator for a study].
- "Risk Assessment". Risk is the potential for an unwanted event to have a negative impact as a result of exploiting a weakness. It can be seen as a function of the value of the asset, threats and vulnerabilities. The process of risk assessment is discussed as part of the University toolkit: http://www.it.ox.ac.uk/infosec/istoolkit/riskassessment/
- "Must" and "Should" indicate requirements and recommendations, respectively. The term "may" is used to indicate that an action is optional.

# 6 Introduction

This document is the Information Security policy for the Cancer Epidemiology Unit (CEU) of the University of Oxford. The purpose of this document is to define Information Security Policy and Procedures within CEU that are compliant with the ISO 27000 series of standards related to Information Security [7], [8], [9] (these standards supersede BS ISO IEC 17799:2005[1] which has been withdrawn). This policy applies to all personnel working at or for CEU at Oxford, regardless of the exact source of their funding. It applies to contractors and other third party entities that may have access to CEU resources. It applies to staff directly attached to the Nuffield Department of Population Health (NDPH), or sub-departments, working on CEU related systems.

## *6.1 What is Information Security?*

Information is an asset that, like other important business assets, is essential to an organisation's work and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown using video or spoken in conversation. Whatever forms the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organisational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the security and work objectives are met.

The CEU Information Security Policy outlines the potential risks to our information, and details the safeguards and procedures that are in place in order to guard against those risks.

## *6.2 IT and Information Security Manager*

### 6.2.1 Responsibilities

Information Security at CEU is the responsibility of the IT and Information Security Manager in conjunction with the Senior Management Committee. The IT and Information Security Manager will:

- provide an approach and framework to implement, maintain, monitor and improve information security;
- provide all CEU staff with guidance on information security through awareness and training;
- assess and address reported security issues;
- establish, maintain and carry out a security incident management process;
- ensure corrective and preventative actions are carried out in a timely manner;

- keep the Senior Management Committee and Co-directors informed of security issues (including all reports of breaches of the Information Security Policy)

### 6.2.2 Contact with special interest groups

The IT and Information Security Manager should maintain appropriate levels of contact with relevant external special interest groups and other specialist security forums or professional associations in order to:

- improve knowledge about best practices
- ensure that understanding of the information security environment is current and complete
- receive early warnings of alerts, advisories, etc. pertaining to vulnerabilities and attacks
- gain access to specialist information security advice
- share and exchange relevant information.

### 6.2.3 External parties

The risks to the unit's information security from external parties should be identified and appropriate controls put in place before granting access to CEU-controlled information and resources. This includes:

- temporary staff
- visitors (including visiting academics)
- students
- maintenance & installation staff
- contractors, consultants, agents & appointees
- collaborators

Where applicable, the external party should sign a confidentiality agreement.

# 7 Asset Management

All assets will be clearly identified and a central inventory of all assets drawn up and maintained. Each asset will have a defined owner.

## *7.1 Software*

A software inventory together with licensing details will be held by the IT and Information Security Manger and regular audits will be undertaken.

## *7.2 Physical*

All physical IT assets will be tagged with a "CEU Computing Item number" sticker and logged in an inventory database by the IT Support Group.

## *7.3 Return of assets*

Employees are required to return any CEU IT assets that they hold on end of contract and to sign a form stating that this has been done. This is verified by the central CEU Administration Group or IT Support, as appropriate. It should be noted that the word "assets" covers both physical and electronic IT assets. It is sufficient to confirm in writing that electronic assets have been deleted or uninstalled. Employees leaving CEU must only retain electronic assets with the explicit permission of one of the co-directors of CEU.

## *7.4 Information classification*

Information within CEU will be categorised as belonging to one of three different classes:

| Class | Access | Examples |
|---|---|---|
| PUBLIC | Not restricted | CEU internet site<br>Published papers<br>Participant information leaflets |
| UNIT | CEU staff and authorized external parties | CEU intranet<br>Standard Operating Procedures<br>Unit policies |
| CONFIDENTIAL | Accessible to named personnel only | Participant details<br>Study databases<br>Papers in preparation<br>Personnel and payroll information<br>Medical information |

For Information held within CEU, all information will be assumed to be UNIT, unless it is explicitly marked as CONFIDENTIAL or classified otherwise in relevant policies or procedures.

Information that passes outside of CEU should retain its classification, unless otherwise explicitly marked. UNIT and CONFIDENTIAL should (wherever possible) be labeled physically or electronically or covered by a suitable transfer agreement. Any information not labeled will be deemed to be PUBLIC. Medical correspondence (including letters to medical practitioners) should conform to Good Medical Practice [5].

Where Third Party access to CONFIDENTIAL information concerning personal details is to be granted, consideration should be given to encryption and contractual confidentiality. A specific "owner" for the information in the third party organisation should be identified where practical.

### 7.4.1 Protection of Information

- Regardless of the classification of information, consideration should be given to ensuring that information is accurate, that changes are accountable and that only authorised individuals can make changes.
- PUBLIC Information, by definition, is in the public domain, and no measures are required to safeguard it from publication or propagation. However, accuracy remains of paramount concern and consideration should be given to ensuring that only authorised information is published.
- UNIT Information is not in the public domain, however, the information is not considered directly damaging and may be transmitted to named external people or bodies. Care should be taken during the transmission of such information to avoid widespread propagation.
- CONFIDENTIAL information is not in the public domain, and uncontrolled dissemination of this information may be damaging to CEU (including, but not limited to, considerations of data protection and good clinical practice). Access to CONFIDENTIAL information should be on a "need to know" basis. Electronic data should be protected by any or all of assigned log-ins, protected network areas and encryption. Physical CONFIDENTIAL information should be kept in locked areas with no general access. The transmission of CONFIDENTIAL information is discussed in Section 10.7.

### 7.4.2 Personal and Sensitive Personal Information

The Data Protection Act (DPA) introduces two definitions:

- Personal Information is information which includes data that can identify a person either explicitly (for example), because it contains their name and address or implicitly (because the data controller has access to other, identifying information (e.g. the electoral roll).

- Sensitive Personal Information is personal information that includes details of the person's health or physical condition; their sexual life; ethnic information; religious beliefs; political affiliations; or criminal convictions.

# 8 Personnel

## *8.1 Job descriptions*

Where appropriate, security and confidentiality responsibilities must be defined in the job description for a role. All personnel must have a confidentiality and security statement included in their contract of employment.

## *8.2 Recruitment procedures*

For CEU employed staff, references including information on previous salary and sickness records are sought before a formal offer of employment is made. The applicant must also complete a rehabilitation of offenders form. During the formal induction process, the new employee will be taken through the Acceptable Use Policy [2] and this policy which they are then required to sign to indicate agreement, understanding and intended conformance.

New employees are on probation and their work is monitored by their line manager or an assigned mentor. Any temporary staff will be vetted generally either by CEU Personnel or by the external agency holding their contract. All temporary staff must sign confidentiality and acceptable use agreements.

## *8.3 Training*

### 8.3.1 General

All CEU staff have access to a wide range of training. Oxford University offers many short courses, which are available to staff. In addition, staff may apply to attend external training courses that are appropriate to their role.

### 8.3.2 Information Security

All CEU staff will be provided with training regarding computer systems and any information security issues that they should be aware of – this includes the reporting procedure for suspected security issues (see Section 13).

## *8.4 Disciplinary process*

Employees who commit a breach of information security may be subject to the formal disciplinary process which may result in termination of contract.

# 9 Physical and Environmental security

### 9.1.1 Physical/equipment security

CEU resides in a secure building with swipe card access on all external doors. External doors are monitored by CCTV. Visitors and deliveries are required to report to the Main Reception for verification by Reception staff. All CEU employees are encouraged to challenge anyone they do not recognise in order to confirm identity and authorisation.

High security areas (e.g. server rooms) are physically and electronically separate from other CEU facilities and have additional security locks in place. Access is restricted to relevant staff. Server rooms have air conditioning units to ensure that the servers operate within operating limits specified by the equipment manufacturers.

Offices are secured by door locks out of normal working hours when not in use.

Protection against environmental and external threats (such as fire, flood and explosion) is covered in the Research Continuity (see Section 14).

Server room power is supplied from multiple mains feeds and, where practical, equipment is split between feeds. Main servers and other key hardware are protected by an uninterruptible power supply units (UPS) in order to maintain service in the event of a power outage and prevent corruption of information.

All CEU staff have access to on-site security staff as well as public emergency services through the internal telephone system. The telephone numbers needed are published on the CEU internal telephone directory and in other locations.

### 9.1.2 Cabling

Data cabling within CEU is, where the fabric of the building allows, contained in trunking or in under floor trays and separated from power feeds. The main data feed to the building is via fibre optic cable.

### 9.1.3 Disposal of IT equipment

Prior to equipment disposal, all confidential information must be securely erased and physically destroyed. A record of the destruction must be logged by IT Support. University and any other relevant regulations on the disposal of IT equipment must be observed.

### 9.1.4 Security of equipment off-site

IT equipment must not be taken off-site without prior authorisation from a member of the Senior Management Committee or IT Support. Such authorisation may be delegated. All devices should be made secure by use of passwords and encrypted data storage areas before removal from CEU. No data on individuals must be taken off site, unless a formal data transfer agreement is in place.

Occasionally, some members of staff may work from home ("homeworking") – see the NDPH Flexible Working Policy [3]. In such cases, it's important to remember that no data on individuals should be removed from CEU, regardless of whether this has been encrypted and/or anonymised. Any employee working from home must discuss the security aspects with their line manager or the IT and Information Security Manager.

Where servers are deployed off-site (to accommodate backup systems for disaster recovery purposes, for example), they will be deployed under equivalent security provisions to the above, with physical access restricted and logical access restricted to CEU staff. Appropriate network controls will be employed to ensure that traffic to and from these servers is protected as if they were part of the CEU network.

See also section 11.2.

### 9.1.5 Physical data records

Confidential Information may be stored in forms other than digital. Such information will be secured when not in use in a locked filing cabinet, locked office or similar. Where such information is stored off site, the storage must conform to CEU standards and must be reviewed regularly.

### 9.1.6 Attached devices

- Devices must not be connected to the CEU internal network without explicit authorisation from IT Support.

- Personal computing devices (definition: section 18.1) must not be connected to the internal network and may be connected to the CEU 'VISITOR' wired network with approval from IT Support. Access to the University's Eduroam wireless network is also provided. Neither wired nor wireless access provides connectivity with local CEU network resources.
- Devices must not be connected to the CEU internal network unless IT Support have administrator/root access, or the analogue for the system in question.
- Any system attached to the CEU internal network (electronically or physically) must be available for prompt inspection by IT Support, without notice. During such an inspection, due consideration should be given to the user's privacy.
- Any device or system found connected to the network that fails these criteria may be disconnected promptly and without notice.

# 10 Communications and Operations Management

## *10.1 Operational procedures and responsibilities*

### 10.1.1 Documented operating procedures

Documented operating procedures should be prepared for all non-trivial system activities (e.g. system start-up and close-down, backup, maintenance, media handling, etc.) and made available to all users who need them.

### 10.1.2 Change management

Changes to systems and application software should be formally controlled. In particular, the following items should be considered:

- Identification and recording of changes
- Assessment of the potential impacts, including security impacts
- Formal approval of changes
- Planning and testing of changes
- Communication of changes to all relevant persons

For individual projects, changes may be logged and tracked using the CEU Bugzilla System.

System-wide changes (e.g. updates to email systems, etc.) will be discussed with the Senior Management Committee, as appropriate.

### 10.1.3 Segregation of duties

Wherever possible, duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of CEU assets.

Wherever possible, separate user identities should be used for live and test systems.

## *10.2 System Planning*

The aim of system planning is to minimize the risk of systems failures. The following items should be considered:

- Performance and computer capacity requirements
- Preparation and testing of routine operating procedures
- Contingency plans and business continuity procedures
- Security controls
- User training

## 10.3 Protection

The IT Support Group will be responsible for maintenance of a CEU firewall, virus protection software and timely installation of security updates to application software.

Software must only be installed on CEU computers by a member of the IT Support.

## 10.4 Backup

Backup copies of information and software must be taken and tested. As well as being stored on-site, regular backups should be stored at a secure location off-site and given appropriate levels of physical and environmental protection (e.g. fire, flood, etc.). At a minimum, backups must be stored in a fireproof, locked safe, with adequate protection on the surrounding building. All backups stored on removable media (i.e. tape) must be encrypted.

The default retention period for CEU data is variable and is set according to the project requirement. This may vary according to local/international regulations.

## 10.5 Network security management

Networks must be adequately managed, controlled and routinely monitored in order to be sufficiently protected from threats and to maintain the security for NDPH systems and applications using the network. This includes information in transit (see section 10.7). Monitoring is discussed in sections 10.8 and 11.5.

Network security is the responsibility of the IT Support Group with the support of the IT and Information Security Manager. However, project based network security (i.e. the appropriate transport of project data) will be the responsibility of the Information Asset Owner for the individual project.

Where sensitive data passes outside of CEU on non-CEU networks or by wireless communication, it should be appropriately secured using approved encryption security (see section 12.3 Cryptography).

## 10.6 Media handling

Physical data storage media should be controlled and physically protected according to its information classification. When no longer required, the media should be destroyed.

## 10.7 Exchange of information

### 10.7.1 Electronic

Exchanges of Unit and Confidential information (section 6.4) and software with other organisations (by whatever means) should be based on a formal exchange policy and should be compliant with all applicable legislation. Procedures should be established to protect information and physical media in transit. Unless impractical, ‘pseudo-anonymisation’, whereby a general identifier, such as an NHS number or full name and address, is replaced with a unique statistical code that has value only to the originators, should be employed.

A variety of agreements are in place covering exchange of information. These agreements vary from organisation to organisation. For example, some organisations require a formally defined transfer mechanism whereas others do not. Unit and Confidential information being sent out of CEU will be secured appropriately (e.g. using password protected documents or complex encryption, as discussed in section 12.3 Cryptography). Any information that is sent from other organisations to CEU should be secured and senders are strongly encouraged to do so. CEU will make available technical help to outside collaborators explaining how to secure information for

transmission.

Emails containing confidential information should use an appropriate form of encryption (discussed in section 12.3 Cryptography).

For any data on any type of media sent from CEU, CEU will bear responsibility for conforming to data protection rules and procedures. Any incoming data will come under the same rules and procedures once acquired by CEU.

Records must be kept for data transferred from CEU using the Data Transfer Records system, held on CEU servers.

### 10.7.2 Mail and courier

Sending information via mail or courier presents a number of problems, primarily because different organisations have different approaches to "best practice". For example, some organisations specify that envelopes must have "private and confidential" on the cover to ensure that only the correct person reviews the information; however, others specify that such labelling must not be used, because it is considered to increase the chance of theft. Study groups within CEU should adopt and document an approach that complies with the following guidelines in this section (whilst also being acceptable to the partner organisations with which they are corresponding and conforms to any other requirements).

- CEU will maintain a list of trusted and reliable courier services. CONFIDENTIAL information should only be sent via a courier on the list. Where practical UNIT and CONFIDENTIAL information should be sent to a named recipient, with only the addressee information visible.
- Where practical, CONFIDENTIAL information should be clearly marked as confidential on the envelope and on the contents (e.g. document, DVD or CD).
- Where practical, "double envelope" systems should be considered (i.e. the media in an envelope marked "confidential" inside a second envelope with the address information).
- Confidential information sent by mail or courier should be sent via a means that allows the package to be tracked and the actual recipient identified.
- Positive confirmation of delivery should be sought (generally via feedback from the recipient).
- Packaging should be sufficient to protect the information from physical damage likely to occur in transit.
- Exchanges of electronic information by courier or mail should also conform to the requirements of section 10.7.1.
- Incoming Confidential mail or packages should be opened away from public areas.

### 10.7.3 Fax

Confidential information should only be sent to a secure fax machine (one for which only approved staff have access). Confidential information should only be sent by fax if neither encrypted electronic nor mail/courier are available or practical. Confidential information should be clearly marked as confidential on each sheet and should not routinely be sent "out of hours" when there is no one to take custody of the information. Where practical, the recipient of confidential information should be informed before transmission and asked to confirm receipt.

### 10.7.4 Oral

Unit and Confidential information should only be provided if the appropriate recipient has been identified. Confidential information should not be left on answer phone or voicemail systems. Care should be taken to ensure that any telephone or verbal communication is limited to those with appropriate access to the information and should not be made from a public area. If in any doubt, the recipient of an unexpected phone call requesting Confidential information should ring back to confirm the caller's identity.

## *10.8 Monitoring*

Systems should be monitored and information security events should be recorded; monitoring is the responsibility of the IT Support Group. Log facilities and log files will be protected against unauthorized access.

All events will be reviewed by the IT and Information Security Manager.

# 11 Access Control

## *11.1 User access management*

### 11.1.1 Registration

A username is unique to any individual with access to CEU systems and must not be re-used. Usernames will not be deleted from the system but will be disabled, when appropriate (e.g. when staff leave). Usernames and passwords are more fully discussed in section 16 of this document

### 11.1.2 Privilege management

Each user may be assigned to one or more roles and will be informed of the rights and privileges associated with that role. Where additional rights and privileges are assigned to an individual, the individual will be explicitly informed. All allocated rights and privileges will be documented.

Changes (including add/delete) to user privileges are made by IT Support and will be logged with documented authorisation for each change.

### 11.1.3 User password management

General password management is discussed in Section 16 of this document. Passwords must be changed immediately if it is believed that the password may have been compromised, and this potential security breach must be reported (see Section 13).

Some applications require an embedded password for operational reasons. These applications must only be run by users who have already authenticated themselves. The access rights of these embedded passwords will only be sufficient for the application to carry out its task and will be reviewed regularly.

Users will be strongly encouraged not to write down their passwords and the use of shared passwords is discouraged unless absolutely necessary. It should be noted that the University IT Regulations specifically ban shared usernames except for “system” accounts.

Any unattended IT equipment will be kept in a locked room, where possible and practical, and where it allows user network access will have password protection. These systems will access central servers on an as-needed basis only. Users must switch off, log out or lock systems when leaving them unattended. Screensavers will be set to password protect login.

### 11.1.4 Review of user access rights

User access rights should be reviewed at regular intervals (and at least annually) and certainly when changing role or project within the department.

## *11.2 Network access control*

All CEU staff will be allowed access to the internal network, which provides access to a file store, network printing and internet connectivity. In addition, users may be assigned one or more CEU or NDPH email addresses and access to the CEU shared drive areas. Further access may be granted as required to specific project.

External access to the CEU internal network is not permitted.

### 11.2.1 CEU networks

The CEU network has a number of VLANs (logically separate networks) and is segregated into two broad sections:

- Internal zone: The main internal network is highly protected by the firewall and is inaccessible from outside. Devices in the internal zone may connect with devices in the DMZ or external devices, provided relevant security precautions are observed.
  The internal zone may be further sub-divided to provide additional segregation through the use of physical or logical networking.
- De-militarized zone (DMZ): This contains externally accessible servers (HTTP, FTP, etc.). The firewall is configured to allow these servers to respond to incoming requests on specified ports only. This zone may be sub-divided either physically or logically to provide segregation for individual servers. Devices in the DMZ must not initiate connections with devices in the internal zone. Devices in the DMZ may initiate or receive connections from external devices.

Data is collected from DMZ servers by processes which are initiated from within the main protected zone.

### 11.2.2 Security

Appropriate security must be employed on the publicly accessible servers to ensure that only desired users have access. This means using the correct protocols. For instance, the main CEU web server will have no restrictions, dispensing pages under HTTP to anyone, whereas web and other servers for particular projects may use HTTPS or SSH. Authentication for other users has already been discussed (10.2.1 and 10.2.2).

### 11.2.3 Externally-managed servers

An externally managed server is one whose day-to-day management is handled by some other than a member of IT Support. Where it is a requirement for a server to be externally managed, the server must:

- Be appropriately segregated from the rest of the CEU network.
- Be managed under the routine provisions of this policy, including the provisions for inspection and control.
- Be regularly audited to ensure that only relevant software is available and that the server is locked down appropriately.

### 11.2.4 Interaction with NDPH

Where devices are attached to the CEU network to support the activities of other NDPH units they must:

- Be appropriately segregated from the rest of the CEU network.
- Be managed under the routine provisions of this policy, including the provisions for inspection and control.

## *11.3 Operating system access control*

### 11.3.1 Identification

Users must identify themselves via username/password and other credentials as appropriate to the method of access. The system will then determine the level of access to system resources based on those credentials.

Access to the main data and statistical servers will only be available once a user has gained access to the network from a PC using the procedure outlined above. Further username/password

access will then be required on a server by server basis. Wherever possible, details of previous logins will be displayed to the user.

Biometric access controls are not currently deemed necessary given the physical and electronic controls already in place.

All passwords will be user chosen and conform to definitions in section 16 and assigned according to section 10.1.1. Passwords will not be displayed in human readable form on computer screens and will be stored in separate areas to data on the associated computer systems. All vendor default passwords will be changed before deployment.

Where possible login attempts to servers will be tracked and logins disabled after a pre-defined number of failed attempts.

### 11.3.2 Security

All system level utilities will be separated from application programs and available to authorised users only by a minimum of separate user ID/login procedures. Some systems only allow access at this level from the system console which will be in a secure room. Servers will have unused facilities removed before use. Terminals unused for a given length of time will time-out to a secure login. No terminal facilities will be available in areas accessible to the general public (i.e. outside of the CEU controlled areas).

Root access to servers will normally be limited to IT Support staff only with individual access identified through an initial individual user login. Root user access will only be used for initial configuration, backups, emergency access to servers and configuration changes (where required). All root level logins will be audited in the system logs.

All CEU staff have access to on-site security staff as well as public emergency services through the internal telephone system. The telephone numbers needed are published on the CEU internal telephone directory.

## *11.4 Application access control*

### 11.4.1 Access restrictions

Application software will usually make extensive use of menu and other pre-programmed techniques for controlling user access to data and facilities. Since many of these applications will be specific to a given study, the controls and restrictions imposed are defined on a study-by-study as well as application-by-application basis. Program development function definitions, together with requirements documentation and extensive testing, will ensure that only necessary information is generated or presented by a given application. Users will be prevented from performing functions for which they do not have authorisation.

### 11.4.2 Sensitive systems

Sensitive systems will normally be restricted to their own hardware / software and hence access will be strictly controlled. Any centrally held sensitive information will have tightly controlled access as well as using encryption (as appropriate) to maintain confidentiality.

## *11.5 System Monitoring*

### 11.5.1 Logging

CEU has a central logging server which captures system logs and some application logs from individual servers. These logs are held for a variable period of time depending on their context and are available for analysis to password protected administrator accounts. Logs are backed up as per Section 10.4 - Backup.

### 11.5.2 Monitoring

Firewall and system logs will be regularly monitored to check for attacks / attack profiles and evidence of unauthorised access. The scope and frequency of these reviews will be based on a suitable risk analysis. These reviews will be performed by IT Support staff or other suitably trained personnel. Other computing activities may be monitored (in accordance with current legislation and the CEU Acceptable Use Policy[2]). Users breaking these Acceptable Use rules will be reported to the Personnel Department for the appropriate action to be taken under the relevant procedures.

### 11.5.3 Time synchronisation

Clocks on all servers and desktop PCs are synchronised using NTP to an internal source timekeeper; in turn, that internal source is synchronised with University of Oxford NTP sources. Where a system is not routinely connected to the internet, other mechanisms for time synchronisation should be used since accurate timestamps are vital for audit trails.

# 12 Systems Acquisition, Development & Maintenance

The very nature of the work done by CEU requires that security is a primary consideration during purchase or development of systems. All projects will identify security requirements in their specifications. If required, the IT and Information Security Manager will advise.

## *12.1 IT systems validation*

IT systems validation is the process of assuring that a computerized system does exactly what it is designed to do in a consistent and reproducible manner. Validation is conducted on the basis of a risk analysis to ensure that systems of higher risk are fully tested. Particular attention is paid to studies in which information is collected and/or stored that might allow identification of individuals.

A validation exercise consists of several formal stages that ensure that quality is built in to the delivered systems, thus reducing any risk to the data and information quality. Software testing forms a valuable part of the validation process and is performed to ensure the correctness, completeness, security and quality of developed computer software. The level and detail of testing should be based on a risk analysis of the systems in question.

## *12.2 Application systems*

### 12.2.1 Input Data

Data input to applications should be validated to ensure that the data are correct and appropriate. This may involve simple or complex validation checks which could include double keying or other verification. On-going reporting of input data will also pick up anomalies missed by input checking. Where hard copy source documents are input into the system, checks will be made to ensure that there are no unauthorised changes to those documents. Each study/group will identify the procedure to use in the event of input check failure. The precise action to take will vary from system to system, as will the responsibilities of the personnel involved, which will also be defined in a standard operating procedure ( SOP).

### 12.2.2 Processing

All processing functions in application systems will be designed and tested to ensure that no data corruption occurs and that data are processed in the correct order. Any failures during the processing phase will be logged and the particular SOP for the project will define the action to be taken. Internal totals and cross checks will be implemented to support the validation of processing steps. Any messages being transferred as part of an application suite will have levels of authentication applied appropriate to the contents and use of the message concerned.

### 12.2.3 Output Data

Any output data will be defined and designed to be correct according to the requirements of the application. Summary and plausibility information will be included where appropriate as a validation on the bulk of the output, together with the use of extensive testing (and regression testing) during development / acceptance. Personnel responsibilities will be defined in the SOP for the particular project.

## *12.3 Cryptography*

Information within the various application systems of CEU will normally be secure because of the other controls and procedures in place. However, there are parts of these systems that are deemed to have confidential data and to be at greater risk than other parts (usually because they are on mobile systems or have to be transferred from one system to another). In this latter case, encryption will be applied to data, messages and (where applicable) software.

### 12.3.1 Policy

It is not practical to mandate a single form of acceptable encryption which will apply in all circumstances. The level and, indeed, the use of encryption will be part of the requirements specification for a given application or part of application.

The specific implementation and technology used will be a combination of the software/hardware design together with guidance from the IT and Information Security Manager, advised as appropriate by relevant CEU committees and the needs of the application.

### 12.3.2 Encryption

CEU uses internationally accepted algorithms for in-house developed applications requiring encryption and/or digital signatures. AES-256 or equivalent is the preferred encryption level and AES-128 or equivalent is the minimum standard. All electronic transfer of Confidential personal information outside of CEU by any means shall be encrypted. When planning a system involving encryption, the regulations and licenses on the export of technology should be borne in mind.

### 12.3.3 Key Management

Where applicable, Public Key[1] techniques will be used with appropriate care being taken of both Public and Private Keys. Suitable logging will take place (this includes tracking of hardware or 'token' authenticators).

### 12.3.4 Digital signatures

Digital signatures[2] will be used where deemed appropriate and where allowed. This will be defined on a case by case basis and will follow CEU and appropriate regulatory guidelines (e.g. Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures [6]) and the needs of the specific application.

## *12.4 Development files security*

### 12.4.1 Control of operational systems

Wherever practical, development and live systems will be segregated. All CEU developed applications should generally be tested and then accepted by the user before live deployment. The

[1] A discussion of public/private key technology is beyond the scope of this document. However, in essence, data may be encrypted with a recipient's public key, so called because it can be made public without harm. The resulting encrypted file can then only be decrypted with the recipient's private key, which the recipient is responsible for keeping secure.

[2] A digital signature is a type of cryptography that gives the receiver reason to believe that the message has been transmitted intact and without tampering, and comes from the claimed source. Digital signatures can also provide non-repudiation.

level and detail of testing should be based on a risk analysis of the system in question, including consideration of how mission critical the system is and the level and extent of confidential information it contains.

The version and patch level of Operating System and third party software will be regularly reviewed, any critical patches or upgrades recommended by the manufacturer will be reviewed by the system owner or nominated IT representative as soon as practicable after release by the vendor and installed if the risk analysis undertaken at this review indicates it is appropriate to do so.

### 12.4.2 Test data protection

Test data should be selected carefully and protected and controlled. CEU will use manual and automated test suites, details of which will be defined within the appropriate project. Any test data will be completely separate from, but representative of, live data. Live data will not be used for application testing unless they have been de-personalised.

### 12.4.3 Source control

Version control systems are available for use. This provides for all necessary control, audit and roll-back facilities.

### 12.4.4 Segregation of Live and Test Environments

Wherever possible, live and developments systems will be segregated and, where this is not possible, steps will be taken to ensure that there is no interaction between the two.

## *12.5 Security in development and support processes*

### 12.5.1 Change control

Formal change control processes must be used during the lifecycle of an application; the processes should be detailed in local project procedures. Change requests for project software must be positively authorised and both the request and authorisation documented. Only specifically nominated personnel within the project are permitted to authorise changes.

All changes must be logged and the impact of the change should be tested prior to system release.

### 12.5.2 Review of operating system changes

Any major operating system changes/patches will be tested before use including testing with key applications. Such major changes will be announced in advance to interested parties to ensure that appropriate procedures take place. Any changes to operational continuity plans implicit in system changes (especially IT Disaster Recovery) will be made as appropriate.

All operating system changes and the testing of these will be logged. The logs will be associated with the actual system which has been changed, apart from desktops where the logs will be held centrally with IT Support.

The level and extent of testing shall be governed by practicality and a suitable risk analysis. In practice, this may mean minimal testing and speedy deployment of security-based updates for Internet-facing systems including desktop PCs.

### 12.5.3 Vendor supplied software modification

Vendor supplied software packages should not generally be modified within CEU; although supplied patches and updates may be applied as recommended. If modifications are required, the vendor should be contacted in the first instance. If the vendor is unwilling or unable to make the modification, then a thorough risk analysis should be carried out by the group proposing the modification in conjunction with IT Support.

Modifications of open source software can also be considered if required: it is considered best practice to submit any patches upstream if this takes place. Any local changesets should be kept under revision control and fully documented.

### 12.5.4 Externally supplied software

All software purchased by CEU will be supplied via a reputable channel (direct from the manufacturer or from a manufacturer's authorised reseller / distributor). All commercial software products will be thoroughly evaluated before use within CEU. Any source code used within CEU but supplied from outside will be thoroughly inspected for quality and embedded illicit software before use. Non-commercial software (e.g. open source, freeware or shareware) should be evaluated in consultation with IT Support. All software obtained externally (whether commercial or not) will be evaluated to ensure its fitness for purpose, including usability, stability, undesirable side effects and documentation.

### 12.5.5 Outsourced software development

CEU does not currently out-source software development. If it were to do so, such development would be on the basis of a formal contract including the stipulation that the third part contractor conformed to this policy.

# 13 Security Incident Management

A system for reporting information security events and weaknesses associated with information systems is in place in order to ensure that they are communicated in a manner that allows timely corrective action to be taken.

## *13.1 Information security events*

Information security events must be reported as quickly as possible. At least one of the following CEU personnel should be informed orally (i.e. not by email, voicemail or written message) to ensure that the recipient is immediately aware of the problem (and avoids, for example, leaving a message for someone who is on leave):

- The IT and Information Security Manager
- A member of IT Support
- A member of the Senior Management Committee

The person informed will liaise with the relevant CEU staff to ensure that

- The event is contained and damage is limited.
- The cause of the event is understood to allow for further analysis and future corrective measures.
- Appropriate documentation is kept.

## *13.2 Reporting information security weaknesses*

Information Security weaknesses (i.e. the potential for information loss or damage) may quickly turn into events (i.e. actual information loss or damage) and so they need to be reported as quickly as possible (as section 13.1).

## *13.3 Management of information security events/weaknesses*

When the event/weakness has been addressed (or as far as it can be addressed for the present time), the IT and Information Security Manager should prepare an "Incident Report" for the Senior Management Committee. The report should include the following:

- Type/details of the event (e.g. software malfunction, breach of physical security);

- Risk/damage to CEU;
- Details of immediate action taken to reduce/eliminate the risk;
- Recommended corrective actions to be taken (which may be short-term and long-term actions);
- Responsibility for the corrective action;
- Timescale for implementation of the corrective action;
- Any relevant additional information.

Note: Corrective action may include legal action so evidence may need to be gathered.

Consideration should be given to the privacy and confidentiality of those involved, either on a personal or professional level. The Incident Report may be "anonymised" when it is considered appropriate. If the incident report would unavoidably contain confidential information, detailed reporting may be restricted.

## *13.4 Guidelines for Handling Illegal Material*

Extreme care must be taken when dealing with allegations of serious misuse of computers, either because criminal or disciplinary proceedings may follow, or due to the presence of indecent images of children (as defined by the Protection of Children Act 1978 and subsequent amendments) or extreme pornographic images (as defined by section 63 of the Criminal Justice and Immigration Act 2008) which may be present on the organisation's computers. Staff investigating such incidents need to act very carefully to avoid harm to their users or potential criminal liability for the organisation or its staff. University guidelines should be consulted in such circumstances: http://www.ict.ox.ac.uk/oxford/rules/soaguidelines.xml

University guidelines exist to ensure that the department's duties of care are met. These duties are to ensure that a serious criminal accusation is referred to the authorities in a timely fashion, but also to ensure that a member of staff does not have their reputation damaged by an unfounded accusation.

In particular, it should be noted that no investigation of a suspected incident must begin until authorisation from the head of department or an authorised deputy is provided. This authorisation must be written in ink (email is not considered sufficient). The authoriser is considered responsible for the management of the incident. The list of authorised signatures is available from the Departmental Administrator and will be supplied to SUPPORT when a new or updated version is made.

If authorisation cannot be obtained, the matter must be referred to the police.

## *13.5 Additional Incident Management Considerations*

The University Information Security Policy [10] contains additional requirements with respect to incident management:

- Information security incidents known to involve the loss or unauthorised disclosure of confidential information held in electronic form, or other serious compromise of core IT infrastructure, must be reported to the Oxford University Computer Emergency Response Team (OxCERT) – oxcert@it.ox.ac.uk. Such reports may be made while investigation is on-going or once complete, as appropriate to the incident.
- Information security incidents known to involve the loss or unauthorised disclosure of personal information held in any form must be reported to the Oxford University Data Protection Officer – data.protection@admin.ox.ac.uk . Such reports may be made while investigation is on-going or once complete as appropriate to the incident. Incidents that have the potential to involve such disclosure may be reported if it is deemed appropriate by the Head of Department or a nominated deputy.

# 14 Research Continuity

The purpose of a continuity and recovery plan is to protect CEU's critical research processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. The plan is not limited purely to information systems; it encompasses other aspects of the CEU's work (e.g. staffing, materials and facilities). As such, information security forms only a part of the continuity of work.

The details of CEU's research continuity and recovery plans are documented by NDPH Central Administration. However, as much of CEU's information is stored electronically, IT Support procedures are in place to reduce the risk and minimise the effect of any such event and to ensure that information required for day-to-day work processes is readily available. This includes protection from viruses, loss of power, intruder access, data backup and stand-by/test systems.

# 15 Compliance

### 15.1.1 Legislation and regulatory requirements

It is outside the scope of this document to list all legislation, guidelines and regulatory requirements applying to all the research organised and collaborated by CEU across the world. However, it is appropriate to identify key legislation and regulatory requirements that apply to many of the activities of CEU. These include:

- EU Clinical Trials Directive
- Data Protection Act 1998 and UK Freedom of Information Act 2000 in the UK (and similar legislation in other countries)
- UK Privacy and Electronic Communication Regulations 2003
- FDA Code of Federal Regulations Title 21 Part 11
- British Standard ISO IEC 17799:2005

Other regulatory requirements or legislation may apply to all or part of a particular study, and details will be found within the supporting documentation of that study.

This policy also complies with

- The NHS Safe Haven Policy (e.g. http://www.leeds.nhs.uk/Downloads/Corporate/FOI/Safe%20Haven%20Policy.pdf)
- University of Oxford Information Security Policy

### 15.1.2 Intellectual Property Rights (IPR)

IPR is a complex area. Queries concerning Intellectual Property Rights should be directed to the Unit Administrator.

### 15.1.3 Data Protection

CEU complies with the UK Data Protection Act and is registered with the UK Data Protection Registrar under the University of Oxford. For international studies, CEU will also comply with the relevant data protection legislation of other countries.

# 16 Policy for Usernames and Passwords

## *16.1 General Notes*

As per the university regulations, usernames, and passwords associated with individual users, must not be shared. Where shared use of a "system level" username (e.g. "root", "administrator") is

required the IT & Information Security Manager shall oversee a register of authorised users and associated usernames.

## *16.2 Usernames*

The following regulations refer to usernames issued by IT Support:

- All CEU members are issued with some form of access to the Windows file system. This will therefore be considered the "primary" reference for usernames.
- New usernames on other systems should be the same as that issued to access the Windows file system.
- The format of a personal username is generally the user's forename. If needed to resolve ambiguity, the first letter of their surname may be added. Additional letters of their surname may be added as required.
- System level usernames (e.g. "root" or a DBA username) should be mnemonic as to their purpose.
- To maintain the integrity of audit trails, usernames must never be deleted from systems.
- Usernames must not be reassigned to another user nor should an individual's personal username be changed.

### 16.2.1 Commissioning Usernames

Access to a resource should normally be requested by the resource owner (e.g. the principal investigator of a study, or similar) of that resource, or a nominated delegate.

### 16.2.2 Decommissioning Usernames

When decommissioning a username, consideration should be given to the following measures. It is noted (and intentional) that some of these measures overlap. Where a user is changing role, then the decommissioning refers to the study resources to which they no longer require access. Where a user leaves their role at CEU, the decommissioning refers to all resources they have access to.

- The user's account should be set to 'disabled', thus preventing all logins.
- The user's email account should be disabled, although with arrangement a suitable "out of office" message can be set if required. Automatic forwarding will not routinely be allowed without agreement of the Senior Management Committee; consideration should be given to whether this might lead to confidential information being transmitted onwards in an insecure fashion.

## *16.3 Passwords*

Passwords associated with usernames must conform to the following rules. Passwords used for other purposes (e.g. protection of files) should conform to the rules as far as practical.

- Passwords must have a minimum of nine characters.
- Apart from password length, all other characteristics of passwords are used to 'score' the password against the various criteria listed below. The total score obtained by a candidate password must exceed the configured threshold. Any candidate password which does not exceed the threshold will be rejected and the user unable to set such a password.
- Passwords containing a mix of character classes (e.g. uppercase, lowercase, numeric characters, non-alphanumeric ASCII characters) will score highly.
- Passwords consisting of dictionary words, simple transpositions of dictionary words or be dictionary words with trivial substitutions (e.g. "0" for "o" or "S" for "5") will score poorly.
- User passwords expire after a period of 180 days; shorter expiry settings may be used.
- Initial passwords (assigned when the account is created) should be pre-expired such that the user is obliged to change the password when first accessing the system.
- The expiry of "system" level passwords should aim to conform to the settings for user level passwords, though differences may be authorised by a member of the Senior Management Committee or a co-Director.
- Passwords must never be re-used; systems will reject any previously-used password.

- Passwords should not be written down or otherwise exposed in non-secure locations.

# 17 Specific Technical Guidance

## *17.1 Use of cookies and similar technology*

Use of cookies should be in line with the current guidance from the UK Information Commissioner's Office. This means that cookies must not be deployed on a user's device without specific consent from the user; the only exception to this are cookies that are "strictly necessary" for a service requested by a user. The example given is that of a temporary cookie deployed to support a "shopping cart" style activity.

Note that the term "cookies" is not limited to HTTP cookies, but should be interpreted to mean any similar technology (such as flash cookies or HTML5 local storage).

To minimise possible compliance issues with any future legislation, studies should only use cookie technology where absolutely necessary.

# 18 Mobile Devices

Use of mobile and personal devices is increasingly widespread, and a number of CEU staff find such devices useful as they offer the facility to work at home or at otherwise unproductive times. However, the use of such devices presents challenges for Information Security as the devices often download emails (and similar) for "off-line" review. This means that should the device go missing and have weak security, there is the potential for information disclosure.

The current version of the policy relates to the connection of mobile and personal devices to the CEU email service and to the University Nexus email/calendar server. There is no current intention of allowing VPN-style access.

This policy proceeds from the principle that access to work email or calendar resources is available for all CEU staff.

## *18.1 Definitions*

- A "mobile device" is a smart phone, iPad or similar device and can include laptops.
- A "personal device" is one that is not owned by CEU.
- "Technical measures" refer to policy points that will be implemented via server settings or similar. Where possible, all policy items will be implemented via technical measures.
- "Procedural measures" are policy points that are implemented via policy, training and audit.
- "Where practical" means that if the device supports the operation under discussion, it should be employed.

## *18.2 Applicability*

This policy is required for mobile devices that fall into one or more of the following categories:

- A CEU-owned mobile device. This is typically a CEU-owned laptop provided for some staff. CEU staff are not issued CEU-owned mobile phones or smartphones.
- A personal device that is expected to contain CEU business-related data. This includes email information that is "synced" onto the device or any documents that are saved locally.
- This policy is advisory for devices that do not fall into the above categories but may be used to review emails or similar via CEU webmail.

## *18.3 Authorisation*

- IT Support may temporarily suspend a CEU user account at any time and without notice if a mobile or personal device is suspected of being a security risk. Any such suspension of

access must immediately be treated as an Information Security Incident and investigated appropriately.
- All staff are permitted to use the CEU email service remotely, however this permission does not imply a "permission to work at home". Refer to the NDPH Flexible Working Policy [3].

## *18.4 Use of Personal Devices*

- Users of personal devices are advised to ensure that work-related email is routed through the CEU email servers and are reminded that personal devices may be subject to inspection as part of a Freedom of Information Act (FOIA) request, DPA investigation or other legal requirement. Work and personal email activities should be clearly segregated where practical.
- Personal devices that are shared with other people must not be used unless their user information is appropriately segregated. This is to prevent unauthorised users from gaining access to CEU resources or information via saved passwords or similar.

## *18.5 General Policy*

### 18.5.1 Technical Issues

Personal devices and CEU-issued laptops must conform to the following:

- Devices must employ a secure password or other secure login approach. Where practical, the password must comply with the general security policy provisions. CEU-issued laptops will have encrypted hard disks with a strong passphrase. Personal devices which are used to access CEU email remotely should have an appropriate unlock code or password.
- Mobile devices must have "timeout" and "lock" facilities. Where practical, timeout settings must be configured consistent with other CEU policy and preferably shorter. Laptop screensavers should be on a short timeout. Personal mobile devices that do not (or cannot) time-out and lock should not be used.
- Device operating systems and other software must be kept up to date with vendor supplied patches.
- CEU-supplied laptops will be managed by CEU IT Support and will be subject to regular, scheduled security audits

## *18.6 Procedural Issues*

### 18.6.1 Security Issues

- Users must report immediately to IT Support the loss of (i) CEU-issued laptops or (ii) personal devices configured to access CEU resources.
- If a user suspects that unauthorised access to the device or data has occurred, the user must report this to IT Support immediately.
- IT Support will refer any security issue to the IT and Information Security Manager for review.

### 18.6.2 General Issues

- Users may download and install vendor supported applications ("apps") onto their mobile device provided those applications do not otherwise conflict with the security policy.
- Users must not store any data on individuals on any CEU-supplied or personal device, whether anonymised or encrypted, under any circumstances.
- Users should also avoid, where practical, storing other confidential information (e.g. unpublished manuscripts) on mobile and on personal devices, and remove such information when there is no longer a requirement.
- Devices must be locked or powered down when left unattended.
- Users should avoid handling confidential data, or entering passwords, in situations where they are vulnerable to "shoulder surfing".

- Users are reminded that confidential information should not be sent by SMS text message.
- Users are responsible for the appropriateness and security of any backup service they employ on their phone. Any backup must be secured as it may contain confidential information.

### *18.7 Supporting comments*

[These comments do not form part of the policy, but are here to explain certain points]

With respect to personal devices, attention should be drawn to the Information Commissioner's Guidance on such: "Information held in non-work personal email accounts (e.g. Hotmail, Yahoo and Gmail) may be subject to FOIA if it relates to the official business of the public authority." Although this article does not touch directly on mobile devices, it is clear that the intent is that "CEU" information held "privately" is subject to the same provisions as if it were on a CEU server.

## 19 References


[1] British Standard ISO IEC 17799:2005 – "Information technology – Security techniques – Code of Practice for Information Security Management"

[2] CEU Acceptable Use Policy – available in V:\IG_policies

[3] NDPH Flexible Working Policy, Ana Fortun (in preparation, March 2015).

[4] University of Oxford Guidelines on the disposal of IT equipment: http://www.ict.ox.ac.uk/oxford/disposal/

[5] General Medical Council, Good medical practice http://www.gmc-uk.org/guidance/good_medical_practice.asp

[6] Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures - http://www.fda.gov/ora/compliance_ref/Part11/

[7] ISO 27000 Information Technology – Security Techniques – Information Security management Systems – Overview and Vocabulary

[8] ISO 27001 Information Technology – Security Techniques – Information Security management Systems – Requirements

[9] ISO 27001 Information Technology – Security Techniques – Code or Practice for Information Security Management

[10] The University Information Security Policy and the "Security Toolkit" is available on http://www.it.ox.ac.uk/infosec